



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,200	10/17/2001	Paul Neil Fahn	06944.0049	4160
27871	7590	06/20/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			KHOSHNOODI, NADIA	
		ART UNIT	PAPER NUMBER	2137
DATE MAILED: 06/20/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/978,200	FAHN ET AL.
	Examiner Nadia Khoshnoodi	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 07 April 2006.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-18 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-18 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 26 October 2005 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/7/2006 has been entered.

Response to Amendment

Applicant's arguments/ amendments with respect to amended claims 1, 7, & 10 and previously presented claims 2-6, 8-9, & 11-18 filed 3/9/2006 have been fully considered and therefore the claims are rejected under new grounds.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamagishi et al., U.S. Pub. No. 2002/0059519 and further in view of Linden et al., U.S. Patent No. 6,360,254.

As per claim 1:

Yamagishi et al. substantially teach a method comprising the steps of receiving a certificate request from a correspondent (par. 66); generating a string for use as a certificate locator (par. 72); utilizing said string to generate said address, said certificate being stored at said address (par. 72 and 205); making said string available for use by said correspondent in generating said address therefrom to retrieve a corresponding certificate from said database (par. 206). Furthermore, Yamagashi et al. teach that in order to create a certificate, certain information is necessary, such as the certificate holder's name, a validity term, and other information as well (par. 16-17).

Not explicitly disclosed is generating a string for use as a certificate locator from information contained in a certificate request. However, Linden et al. teach generating a URL for access to private information, where the token used in the URL is derived from a user identifier and a time variable (col. 4, lines 61-65). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Yamagishi et al. to generate the string for use as a certificate locator from information contained in the certificate request. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Linden et al. suggest that the string ("token") should be generated from the user identifier and a time stamp in order to further protect against unauthorized identification of valid tokens in col. 4, lines 57-65.

As per claim 2:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 1.

Furthermore, Linden et al. teach the method wherein said string is mapped to an address in a directory (col. 4, line 65 – col. 5, line 2).

As per claim 3:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 1.

Furthermore, Linden et al. teach wherein said string is used as said address in said directory (col. 6, lines 51-65).

As per claim 4:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 1.

Furthermore, Linden et al. teach the method wherein a mathematical function is applied to said information to obtain said string (col. 4, line 65 – col. 5, line 2).

As per claim 5:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 4.

Furthermore, Linden et al. teach wherein said mathematical function is a hash function (col. 4, line 57 – col. 5, line 2).

As per claim 6:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 5.

Furthermore, Linden et al. teach wherein said string is a portion of the output of said hash function (col. 4, line 57 – col. 5, line 2).

As per claim 7:

Yamagishi et al. substantially teach the method comprising the steps of preparing a set of information for inclusion in a certificate request (par. 66), forwarding said string to said recipient to enable said recipient to generate said address therefrom, wherein said address indicates the location of said certificate in said database for subsequent retrieval by said recipient (par. 205-206).

Not explicitly disclosed is generating from said set of information a string for use as a certificate locator in a database at said address. However, Linden et al. teach generating a URL for access to private information, where the token used in the URL is derived from a user identifier and a time variable (col. 4, lines 61-65). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Yamagishi et al. to generate the string for use as a certificate locator from the set of information contained in the request for a certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Linden et al. suggest that the string (“token”) should be generated from the user identifier and a time stamp in order to further protect against unauthorized identification of valid tokens in col. 4, lines 57-65.

As per claim 8:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 7. Furthermore, Linden et al. teach wherein said information includes a time varying element (col. 4, lines 60-65).

As per claim 9:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 7.

Furthermore, Linden et al. teach wherein said mathematical function is a hash function (col. 4, line 57 – col. 5, line 2).

As per claim 10:

Yamagishi et al. substantially teach a method comprising the steps of collecting at one of said correspondents, information comprising a request for a certificate of said certificate authority (par. 66 and par. 204), forwarding said request to said certification authority (par. 66 and par. 205), generating an address from said string at which said certificate is to be stored (par. 205-206), storing said certificate issued from said request in a database at said address (par. 72 and par. 205), and forwarding said string from said one correspondent to another of said correspondents to permit retrieval of said certificate from said database at said address (par. 205-206).

Not explicitly disclosed is the method comprising computing a string from said information comprising said request for use as a certificate locator by said one correspondent and said certification authority. However, Linden et al. teach generating a URL for access to private information, where the token used in the URL is derived from a user identifier and a time variable (col. 4, lines 61-65). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Yamagishi et al. to generate the string for use as a certificate locator from the set of information contained in the request for a certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Linden et al. suggest that the string (“token”) should be generated from the user identifier and a time stamp

in order to further protect against unauthorized identification of valid tokens in col. 4, lines 57-65.

As per claim 11:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach wherein said information includes a time varying element (col. 4, lines 60-65).

As per claim 12:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach wherein communication between said one correspondent and said certification authority is performed over a secure channel (col. 8, lines 25-53).

As per claim 13:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach wherein said other correspondent obtains an address of said certificate from a known address of said database and said string (col. 3, lines 56-65).

As per claim 14:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach the method wherein said other correspondent forwards said locator to said certification authority for construction of said address (col. 3, lines 46-65).

As per claim 15:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach wherein said string is computed by application of a cryptographic hash function at least part of said request (col. 4, line 57 – col. 5, line 2).

As per claim 16:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 15. Furthermore, Linden et al. teach wherein said information includes a time varying element (col. 4, lines 60-65).

As per claim 17:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 15. Furthermore, Linden et al. teach wherein said string is a portion of the output of said hash function is used as the string (col. 4, line 57 – col. 5, line 2).

As per claim 18:

Yamagishi et al. and Linden et al. substantially teach the method according to claim 10. Furthermore, Linden et al. teach wherein said bit string is utilized as a pointer to an address in a directory (col. 4, line 65 – col. 5, line 2).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,959,308
2. US Patent No. 6,438,690
3. US Patent No. 6,795,920

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Nadia Khoshnoodi
Examiner
Art Unit 2137
6/13/2006

NK



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER